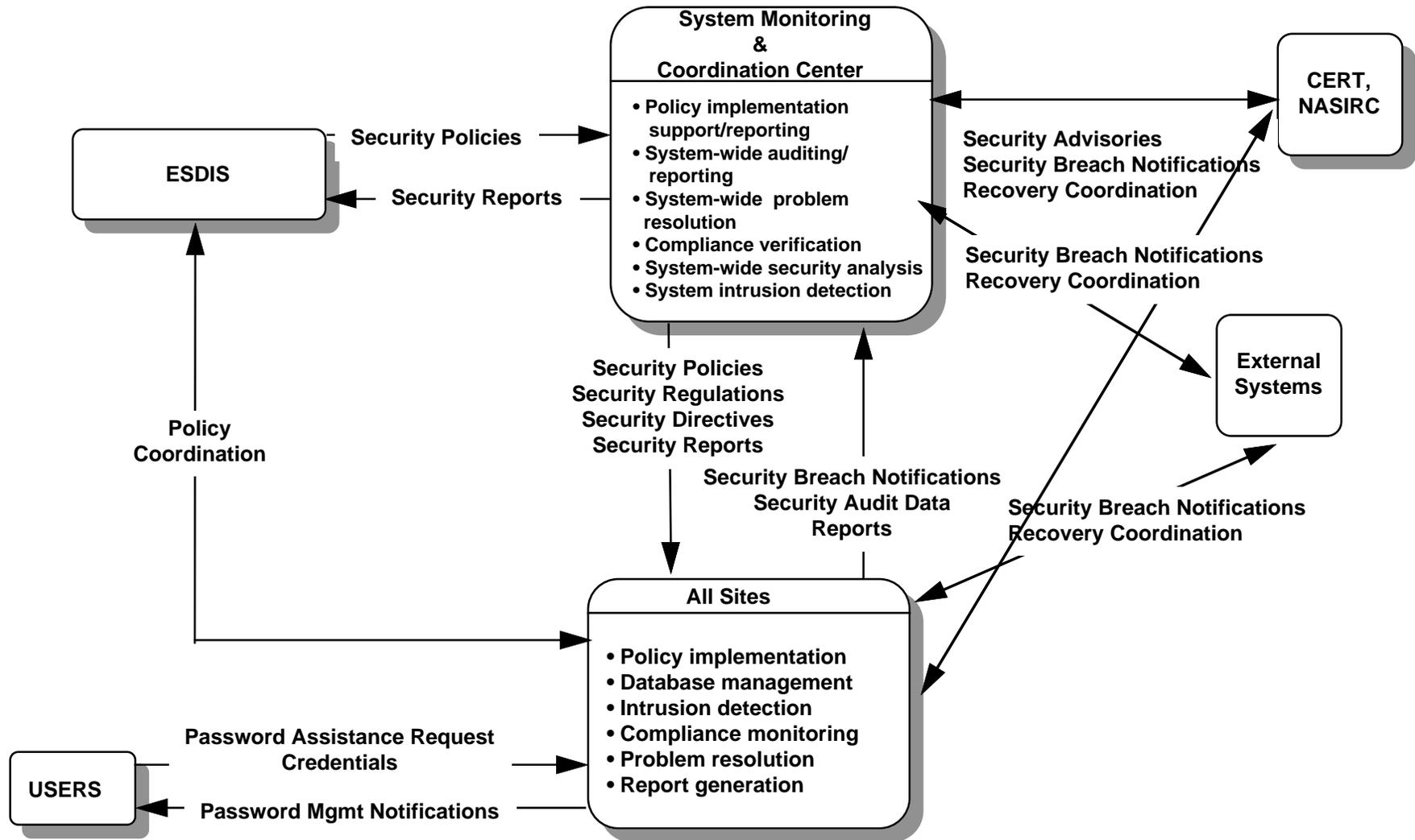


# Security Management: Scope

- **Security database management**
  - Authentication databases
  - Authorization databases
- **Compliance Management**
  - Password policy (length, lifetime, guessability, etc)
  - File/directory permissions
  - Filesystem Integrity
- **Intrusion Prevention/Detection**
  - Detection of viruses, worms and Trojan horses
  - Excessive login failures
  - Unauthorized access to ECS resources
- **Security Event Resolution**
- **Report Generation**

**NOTE:** The Data Integrity & Data Privacy (Release B) Services have only software interfaces, and none for Operations Security Audit Information Collection is addressed in Accountability Management.

# Security Management: Organizational Interfaces



# Security Management Roles

## ESDIS Management

- Establishes and reviews Security Policies

## DAAC/SMC Management

- Adapts site/system security policies and procedures
- Interface with external security agencies (e.g. CERT and NASIRC) for security advisories and incident reporting
- Reviews site/system security analysis
- Approves security problem resolution
- Verifies compliance to policy

## SMC - Security Administration & Analysis (off-line/on-line)

- Disseminates ECS security policies and procedures (off-line)
- Maintains SMC security databases (off-line)
- Monitors system-wide security events (off-line)
- Performs system-wide security analysis (off-line)
- Coordinates recovery from security problems with DAACs and external systems (off-line/on-line)

# Security Management Roles (cont.)

- Reviews system-wide security problem resolution (off-line/on-line)
- Generates system-wide security reports (off-line/on-line)

## DAAC - Security Administration & Analysis (off-line/on-line)

- Implements ECS and local security policies and procedures (on-line/off-line)
- Maintains site security databases (off-line)
- Monitors site security events (on-line)
- Performs site security analysis (off-line)
- Coordinates recovery from security problems with other DAACs/SMC/external systems (on-line/off-line)
- Verifies local security problem resolution (off-line/on-line)
- Generates local security reports (off-line/on-line)

## User Services/User Help Desk

- Provide an interface for Users in reporting security access problems/comments

## Users

- Report security access problems

# Security Management: Process

- **Establish and maintain:**
  - **Policies for compliance management, reporting**
    - » **Password policies may be customized based on user groups and affiliations**
  - **Standard operating and analysis procedures**
- **Establish and manage security databases**
- **Verify compliance to policy**
  - **Tests (e.g. password audits) run on scheduled and on-demand basis**
- **Check for Intrusions**
  - **Tests (e.g. virus checks) run on scheduled and on-demand basis**
  - **Security analysis capabilities as provided by available COTS products**
- **Coordinate recovery from incidents**
- **Generate reports**

# Security Management: The Tools

Activity	Tools Available/ Candidate COTS	Functionality/Capability Provided
Establish policy	Authentication databases All ECS servers (custom)	Password guidelines Login failure guidelines Inactivity timer guidelines
Database Management	DCE Registry Database Host Authentication DBs DCE ACL Managers Router Configuration DBs	Authentication Authorization
Compliance Management	COPS, CRACK, TRIPWIRE, FORTRESS	Password auditing File system integrity checking
Intrusion Detection	COTS & Custom	Viruses, Worms, Trojan horses, Breakin attempts
Event Resolution	Standard Operating Procedures	Recovery procedures
Report Generation	COTS TBD, RDBMS	Standard and ad-hoc reports